Digitalizing the World: The Era of Invisible Power

Thomas Flichy de La Neuville (Rennes School of Business)

Introduction

It is clear that the digitalization the world, which interconnects people and equipment, represents a major civilizational transition. It is changing the ways in which power is exercised, partly concealing it from public view. Hackers operate anonymously, attacking websites that collect unwitting users' information.[1] The cybernetic era is therefore making power less perceptible and this, in turn, makes research into this current technological shift crucially important.[2] However, this endeavor is not without risk. There is a danger that we mistake advances in digital technology for the true vitality of a civilization built on the ability to breathe new life into every part of society.[3] Currently, the real and virtual worlds are hybridizing, generating fears around human life being stripped away in favor of technology. This concern is balanced out by hopes that a form of digital humanism will arise. Still, the situation is difficult, because invisible power is not easy to spot.[4]

Indeed, one of the dilemmas faced by research into cybersecurity is that most data is not accessible to the wider public. This complex field of study can only be deciphered using the technical capabilities of the army or intelligence services. Still, it is possible to overcome this barrier by exploring the sources of information at either end of the chain. Upstream, a small number of philosophers are reflecting critically on the digital world. One example is Bernard Stiegler, who considers that the internet is a disruptive technology, in that digital

[1] The idea behind all anonymizing systems is to blend various network users' communications together so that they become individually indistinguishable. As a result, it becomes impossible to draw a correspondence between data and identity.

[2] Cyberattacks have now become so sophisticated that it is impossible to determine where the perpetrators are located. This makes it difficult to implement aggressive tactics as recommended by the latest cyber strategy white paper.

[3] Arnold Toynbee wrote that "if we were to look at the history of war techniques in isolation in Greek history, we would observe continuous progress from beginning to end, before, during and even after the growth period. We would also observe that each step on the road to progress is stimulated by events that are otherwise disastrous for Hellenic civilisation." Toynbee, *L'histoire* (Paris: Gallimard, 1951), 219. Translation from the French text.

[4] The wider public is entirely unaware of how Google's search engine works.

automation leads to tax avoidance and unemployment.[5] Eric Sadin, meanwhile, defines artificial intelligence (AI) as a kind of rationality that interprets various situations in real time in order to continually propose services and products, a technoliberalism aiming to mould behavior. Lastly, Kave Salamatian sees the internet as a many-tentacled beast with a hyperconnected heart, whose underwater infrastructure provides an indication of the state of digital geopolitics.[6] Downstream, various blogs and websites testify to the current vitality of technology. It is useful to cross-reference technology website Wired.com, which is written for a nonspecialist audience, with French websites InternetActu.net and Reflets.info, which offer a more critical reading of the subject.

Various online tools also enable us to assess the evolution of digital technology, from maps of the underwater cable network that carries 99 percent of internet data to maps of the users of TensorFlow or Shodan.io, which provides an overview of connected devices.[7] It is also possible to approach the gamer-hacker community, which is not opposed to talking about its underground activities (although IT specialists can be reluctant to come into contact with a world quite different from their own).[8] However, neither upstream nor downstream information sources are location-specific. As a result, monitoring software such as Tadaweb.com and relational mappers such as Gephi.org give us an idea of digital geopolitics in specific places. Counterintuitively, the enhanced imperceptibility of digital power does not tend to smooth out the idiosyncrasies in connected individuals' data. Digitalization thrives by collecting personal data on a massive scale and this, in turn, means breaking societies down into preidentified microgroups. Enclosing groups of individuals into online silos is a

[5] For her part, magistrate and cyber specialist Myriam Quéméner examines how French law is changing in reaction to disruptive digital technology.

[6] The Suez Canal and Strait of Malacca are strategic points for underwater cables. China, meanwhile, is only connected to the world via four points.

[7] The Marea network is made up of cables no bigger than a hosepipe and was completed in 2017. It links Virginia to Bilbao and currently transmits 75 percent of the world's current online traffic.

[8] The website Pastebin, for instance, lists the most recent hacking operations. See also Tim Jordan and Paul Taylor, "A Sociology of Hackers," *Sociological Review* 46, no. 4 (November 1998): 757–80. Note that people with Asperger's syndrome (a form of autism characterised by communication difficulties) are particularly likely to thrive in IT professions. Steve Silberman, "The Geek Syndrome," *Science*, January 12, 2001.

prerequisite for effective personalized marketing, of which electoral marketing is an offshoot.[9] Paradoxically, when human societies are digitalized, their identities become more distinct, to the extent that microgroups of connected but single-minded individuals find themselves in opposition to one another.[10] Pay close attention to it and the permanent connectivity generated by all-governing algorithms appears more belligerent than unifying.[11] To understand this, we have to examine the digital revolution's workings so that we can sketch out the potential geopolitical consequences.

The Commercial Dynamics of the Digital Revolution

Driven by an ambition to replace human unpredictability with artificial intelligence, the digital revolution uses captology to monopolize consumers' attention and has remained largely untouched by cyber-dysfunctionalities.

Artificial Intelligence: A Trojan Horse Designed to Rob Humans of Their Independence

In the years to come, the development of artificial intelligence will be flanked by the development of 5G and quantum computing. 5G is one hundred times faster than 4G and interconnects people with digital devices, providing the conditions for everything from smart cities to automated environments. 5G is designed for the Internet of Things, such as smart cars and drones, for example. Switzerland has taken an early lead in this area, launching 338 5G masts on April 17, 2019. This technology is not without its risks, however, as it must be relayed every 800 meters. The waves are very high in frequency and noncontinuous. The situation is further complicated by the fact that China has a number of 5G-related patents,

[9] One of Quantcube Technology's flagship products is Global Macro Smart Data, a real-time predictive platform licensed annually to users. Since May 2013, Quantcube Technology has predicted twenty-one election results with 92 percent accuracy, several weeks before the polls even opened. The start-up notably predicted that the UK would vote to leave the EU in 2016 and that Donald Trump would win the 2016 US presidential election (a fortnight ahead of time in the latter case), as well as the results of France's first round of presidential elections in 2017 and the 2018 American mid-terms.

[10] Major digital platforms' most significant means of reducing friction between these different identities is to moderate users' posts. This invisible task was analyzed by Tarleton Gillespie in *The Custodians of the Internet* (New Haven: Yale University Press, 2018), 296. It consumes a huge amount of resources. Global platforms use automated detection tools to moderate content. The task of moderation itself involves flagging up offensive or inappropriate content.

[11] Unless, of course, these virtual confrontations threaten the cyber security upon which foreign investments depend.

with obvious geopolitical implications. In May 2019, US president Donald Trump banned American telecoms networks from buying Huawei equipment. Indeed, the United States has expressed fears about wide-scale espionage and has pressured its allies to freeze out the Chinese company. However, should Huawei and other Chinese businesses be prevented from rolling out 5G capabilities in Europe, the cost to European telecoms operators would be €55 billion and eighteen months of lost time.

On the quantum computing side, new quantum computers (and IBM Q in particular) are rendering current cryptographic protocols obsolete. While the ten or so quantum computers currently in existence are still in the experimental stage, in the next few years, the development of AI will primarily allow it to not only guide consumers' choices but also to reform state bureaucracy.[12] A new science – captology – has been developed to this end.

Captology: The Art of Invisible Manipulation

AI is first and foremost about emotions.[13] Algorithms turn our mental space into code in an effort to capture our attention. The origins of captology reside in the work of Stanford University's B. J. Fogg, who published *Persuasive Technology: Using Computers to Change What We Think and Do* in 2003. Persuasive technologies have been designed by choice architects to nudge people's choices in a certain direction. Rooted in behavioral economics and neuro-marketing, they lend algorithms a governing power. This new economy considers our attention spans to be a rare and precious resource that can be used to a business's advantage when it is focused on information that, in turn, provokes a particular action. Recognizing the potential negative effect of these techniques, Bernard Stiegler has criticized psychotechnology that short-circuits our attention spans, as had Noam Chomsky and Edward S. Herman before him when they denounced the media's role in manufacturing consent.

[12] State start-ups could find themselves at the cutting edge of government reforms.

[13] For Pierre Bellanger, "software and algorithms are human thought in code. Only a third of our brains is dedicated to rational cognition. If the majority of our thoughts emerge from our unconscious, as soon as networks develop they become unmoored from reason, control and any understanding of our own thoughts. The internet is coding and connecting up our dreams." Translation from the French text.

Captology can also builds on artificially generated anxieties, such as the “fear of missing out.” This particular fear is largely fueled by certain aspects of modern technology, such as mobile phones and social networking sites, such as Facebook or Twitter, which enable users to constantly compare their profiles. As the world’s internet usage grows, a proportion of individuals will become psychologically dependent on being online and suffer from anxiety whenever they are not logged in.

Captology’s potential for generating negative outcomes within the context of global digitalization is clear–and yet in the imagination of the global citizenry and security services it is overshadowed by fear of cybercrime, which, however, tends to be overemphasized in the surrounding discourse.

Cybercrime’s Minimal Impact on Global Digitalization

Although cybercrime is becoming increasingly prevalent, especially in developing countries, groups of hackers rarely manage to paralyze organizations or states for long periods of time.[14] In reality, cyberattacks (which are often supported by states) are a sophisticated version of three ancient practices, namely *sabotage, espionage,* and *subversion*.[15] Although the costs involved in these operations have plummeted, cybersabotage is still limited in scope. Still, it has been shown capable of doing damage in various ways: it is now possible to blow up a pipeline, break a dam, scramble a radar, delay a nuclear program, shut down a bank, take control of a car or assassinate someone by booby-trapping their mobile phone.[16] Cyber-espionage is the real growth area: today, spies are overwhelmed by the amount of stolen data on offer, rendering them incapable of interpreting all this information shorn from its cultural

[14] Cybercrime is mostly fueled by developing economies, which have recently become a significant force as far as fraud is concerned. Attacks originating in Brazil continue to rise, making it one of the world’s five most prolific cybercrime hotspots. Currently, the most effective hackers operate from Israel and India.

[15] The Tor network, which is spreading through the darknet, uses the onion routing technology that was developed by the US Navy in the 1990s. This military technology was mostly financed by the US government to promote democracy around the world. Until 2017, the US government funneled nearly all its funding via the US Navy, the State Department, and the Broadcasting Board of Governors that emerged from the CIA. As a result, major intelligence agencies can reverse data anonymizing processes to uncover Tor users’ true identities.

[16] Hackers can control the automatic windows and the indicators on a dashboard, or even cause the engine to malfunction.

context. In the world of espionage, attacks are becoming increasingly sophisticated. Certain viruses erase themselves as they go, for instance, making them impossible to trace.[17] They can also mutate, just like biological viruses.[18] As for subversion, while it is easy to start a protest movement online, it is very difficult to maintain in the long run. As a result, sabotage makes it temporarily trickier for the world to go digital, whereas espionage harvests the results of our constant connectivity. Ultimately, only noncommercial subversion is capable of endangering the current digital transition, but it is too infrequently executed to pose any serious kind of threat.

Having examined the digital revolution's workings, we can now sketch out the potential geopolitical consequences. Indeed, as can be seen from the preceding discussion, global digitalization is rooted in market dynamics and enables power to be exerted invisibly upon connected individuals. From a broader standpoint, it is aiding financial capitalism maneuver toward a new international geopolitical configuration, to which we now turn.

Digital Empires vs. Digital Vassal States

Geopolitics in the digitalized world are characterized by three major trends: an erosion of American power, an increase in Chinese power, and competition between the two to digitally colonize the rest of the world.

Eroding America's Digital Power

American power entered the virtual world via an oligopoly: GAFAM. Made up of five major businesses (Google, Apple, Facebook, Amazon, and Microsoft) and founded by former hackers,[19] GAFAM physically stores information.[20] As such, this big data is accessible to the

[17] According to Kaspersky Lab's predictions for targeted threats in 2019. The next viral infections will be imperceptible.

[18] Viruses use an unstable enzyme to multiply. Because there is no corrective system to call upon, this error remains in the genome. It occurs in about one out of every 10,000 cases. Much variation therefore exists within a viral population.

[19] Examples include Steve Jobs (Apple), Mark Zuckerberg (Facebook), Bill Gates (Microsoft) and Linus Torvalds (Linux).

United States and its British relay station. 80 percent of data goes through the United States, and listening stations are positioned close to where underwater cables reach land.[21] The geopolitical implications for control over cables range from fostering dependency among overseas territories far from major population centers,[22] rising Chinese-American tensions,[23] and in other, less-publicized arenas such as Portuguese-Brazilian wrangling for control over the former Portuguese colonies' economic market.[24] Most notably, in response to US dominance other actors have increasingly taken countermeasures: For example, to evade American surveillance, Brazil has built its own cable link to Spain. Similarly, China has built the Sea-me-we 5 cable to connect with the Middle East and, ultimately, Europe. And the Huawei Marine group is laying more and more underwater cables, for instance between Brazil and Cameroon.

Because GAFAM behaves like a state, Denmark dispatched an ambassador to it in 2017. In reality, it is more like a kleptocracy, which is living off stolen data, and whose hybridized belief system borrows from both left-wing libertarianism and right-wing technological determinism.[25] The resulting techno-libertarianism is espoused by visionary, charismatic founders who generate innovative commercial offerings that are always technologically avant-garde. With support from investment funds, GAFAM spent $58 billion on research and development in 2016. They partly owe their monopoly to the brilliant Chinese

[20] The internet's infrastructure is mainly made up of high-capacity underwater fibre optic cables linked up to terrestrial cables and routers. For Europe, the most important cables are those that link the continent to the UK and, from there, to the US via the Atlantic Ocean.

[21] Historically, underwater cabling helped the British Empire to increase its financial power. The first functional cable was laid in 1851 between the coasts of France and England with the primary aim of telegraphing stock market information. Today, the Seaborn Networks consortium has now started building an underwater fibre optic connection between Fortaleza in Brazil and Wall Street. Known as Seabras-1, the project will eventually link up to African financial markets via South Africa.

[22] New Caledonia has been linked to Australia via the Gondwana-1 cable since 2009, guaranteeing it the fastest possible communications. Orange is also planning to link French Guiana to the Caribbean.

[23] The United States has responded vigorously to increasingly powerful Chinese investments. In 2013, the American administration thwarted plans to lay a new transatlantic cable between New York and London, to which Chinese firm Huawei was meant to contribute.

[24] The SACS cable has linked Angola to Brazil since February 2019, while ELLALINK connects Portugal to Brazil via Cape Verde.

[25] GAFAM's system bears historical comparison to the extremely mobile Venetian gondolier company, which was able to pass information shared by travelers to the doge.

and Indian minds that staff Silicon Valley. They are still in competition with China, however, which is trying to prevent them from developing any further.[26] To maintain its dominant position in this environment, the United States must speed up its industrial integration with Europe. For its part, if it hopes to reestablish its digital sovereignty, Europe needs to redouble its own efforts and investments in digital technology.[27] If it does not, it will have to accept strategic alliances which reduce it to nothing more than a digital vassal state.

China's Rise to Cybernetic Power as an Indicator of Rare Resources

China's demographic collapse has forced the emerging power to concentrate on technology. The PRC is now hugely connected, and over half of its population has been online since 2017. Four hundred million Chinese people play online games, for example. Chinese internet users are online for about three hours a day, and over half of that time is spent on a mobile device. They browse and watch online videos, abandoning TV screens in favor of more nomadic options. Within this context, as part of its attempt to encourage digitalization while safeguarding against domestic political change, China is seeking to disentangle itself from ICANN, a legal authority based in California that regulates the internet, by boycotting multilateral meetings. Its objective is to draw a strict dividing line between the "Chinese internet" and the "global internet." In an attempt to "cleanse" the internet, the Chinese Communist Party has long sought to strengthen its grip on what it describes as information pollution and "electronic opium."[28]

From another angle, the Chinese have outclassed the Americans when it comes to AI. AI thrives when data is collected in massive quantities, and China has huge amounts of homogenized data that enables it to outstrip the United States in this realm. The country's

[26] There are similarities between China's efforts and the way the United States attempted to block the USSR's forays into the nuclear and aerospace industries in the 1950s.

[27] It should be noted, for example, that despite its legal stability and general appeal, France has not been able to create any ground-breaking innovations within the technology realm for the past twenty years due to its rigid labor laws.

[28] Internet addicts are viewed as both "deviants" who need their behavior corrected and "sick patients" who require medical help.

"social credit" system, which awards every citizen a certain number of points based on behavior, has enabled it to extract vast amounts of data since it came into force in 2020.[29] Two modes of plundering data are thus going head-to-head: GAFAM pilfers our data on the one hand, while the Chinese government pilfers its own citizens' data on the other. The Chinese have the data but the Americans have the algorithms, which is why it is so crucial to the Chinese that they manage to plunder the latter or attract the very best engineers who will help them catch up. Competition here is fierce and has left behind India, which is only responsible for developing existing programs. For example, in order to maintain its digital independence, China restricts how its rare metals are exported and used, as these will go on to be used in the mobile phone manufacturing process. For Guillaume Pitron, the battle for rare metals is the hidden side of the digital revolution, and in the future, tensions will become particularly high in territories targeted by cyber-colonists.

Major Powers Competing to Digitally Colonize Africa

If the digital colonisation process were modeled on an algorithm, it would include the following steps. First, the colonizer would facilitate a cyberattack on the target state's communications and present itself as the latter's savior. Next, it would connect the country to the internet, secure its strategic networks and capture local cyber elites by rolling out a master's degree program in digitalization. It would then pillage the country's data, take over the consumer market and, finally, engage in online electoral marketing to maintain its grip on its conquered market.

This is precisely what is happening in Africa, where connectivity is growing rapidly. In 2018 alone, 35.2 percent of Africans were using the internet, compared with 16 percent in 2012. In this context, China has taken a very original stance toward the continent. First of all, Chinese businesses have provided the continent with technological tools at very competitive prices. For instance, Shenzhen-based electronics manufacturer Huawei has been operating in

[29] This system is based on the questionnaires used by certain American insurance companies.

Africa since 1999. In 2013, it partnered up with Microsoft to conquer the African smartphone market and is now outperforming the Californian giant in this sector in Africa. Huawei's ambition is now to sell premium telephones to an African middle class looking for enhanced services, further positioning China as a leader in this market. There are, however, significant differences between countries, from North Africa to the Sahel region, as the Chinese are not the only cyber colonizers in town.[30]

For example, the British are also taking an interest in this promising market and organized a cyber-forum in 2018. France, too, has been seeking a piece of the pie. In 2019 Orange set up a specialist cyber defence subsidiary in Morocco: Orange Cyberdefense Morocco officially opened for business in Casablanca on April 16, 2019. A master's degree in cyber defense has been set up in partnership with the Université Polytechnique Hauts-de-France in Valenciennes to attract African talent and launch their careers. France also has a long-established presence in Libya as, in 2007, Amesys—a French subsidiary of Bull—sold its Eagle program to the Gaddafi regime to track its opponents. After changing its name to Advanced Middle East Systems, the company then sold a similar system to Egypt known as Cerebro. In the Sahel region, practices are changing, as internet cafés offer faster internet speeds rather than access to computers, suggesting rapidly progressing digitalization. The French army ran several cybersecurity courses, including in Nouakchott, Mauritania, from September 10 to 13, 2018, and in Niamey, Nigeria, from January 29 to February 3, 2018.

The Middle East: Digital Islands and Rich Pickings

Finally, it is worth considering here another region where digitalization is taking on increasing geopolitical importance–the Middle East. The latter has two digital "islands," Iran and Israel, which represent opposing yet mirroring forces. On the one hand, Israel provides 7 percent of the world's cybersecurity, and its industry benefits from high levels of investment

[30] For example, Algeria – considered the least secure country—had to call in specialist cyber police officers to monitor its baccalaureate exams in 2017.

that aim to protect a territory stripped of its strategic importance, while also improving its ability to export innovations.[31] On May 6, 2019, Israel sent out a warning to hackers operating outside its borders. After one cyberattack in particular, the Israel Defense Forces bombed a building in the Gaza Strip that was sheltering Hamas hackers. This has not prevented Israel itself from recruiting hackers keen to offer it their services for a hefty fee.[32] The field is growing, as exemplified by three former Israeli intelligence officers who founded XM Cyber in 2016 to operate in this particular field. For its part, and in opposition to Israel, stands the digital island of Iran, a country with equal levels of creativity but lacking in Western investment.[33] Among other things, Iran appears to have been behind cyberattacks on certain British banks in December 2018. The viruses used—Shamoon 1, 2, and 3—also targeted petroleum infrastructures in the Gulf's oil monarchies.[34]

Yet, Iran and Israel are not the only actors in the Middle East whose digitalizing activities have an impact outside their own borders. In Turkey, the nationalist Cyber-Warrior Akıncılar group has hacked anyone or any organization deemed opposed to the interests of Turkey and Islam.[35] Saudi Arabia, meanwhile, has enjoyed technical support from certain Israeli cybersecurity firms, which have made use of their position to gather data on the behavior of the country's elites or opponents to the regime.[36] Still, despite the protection offered by these Israeli companies, Saudi Arabia is now the most frequently targeted Middle

[31] $800 million in 2017.

[32] Hackers are highly coveted. In fact, Dubai has even organized a hacking fair!

[33] The word "algorithm" was invented by Persian mathematician al-Khwarizmi in the ninth century.

[34] Cybercrime can sometimes be a proxy for military action. This was the case for these Iranian cyberattacks, which were designed to relieve pressure on the country during the embargo.

[35] They hacked into *Charlie Hebdo*'s website, for instance, in 2011.

[36] In 2017, representatives of the Herzliya-based NSO Group Technologies held a series of meetings in Vienna and at least one Gulf nation, during which a $55 million contract was signed to supply Saudi Arabia with its famous Pegasus spyware. On the opposition side, Jamal Khashoggi and Omar Abdulaziz wanted to set up a cyber-opposition movement.

Eastern country when it comes to cyberattacks, which mostly aim to steal information from private and public institutions' information systems.[37]

Conclusion

The growth in digital power offers a very imperfect reflection of the real clout of the states under discussion here: GAFAM's rise obscures the United States' geopolitical decline, while China's technological power conceals its demographic fragility. Conversely, in both Africa and the Middle East, hacking operations designed to steal digital or financial resources reveal the weaknesses of supposedly powerful forces.

Social digitalization rates are therefore a better reflection of the resources that are immediately available rather than their future potential. The internet has become a bitterly contested space among competing economic powers. The aim of this competition is to effectively privatize a space that is temporarily free for users to explore. Permanent connectivity, which devours instant data and interconnects objects and reified human beings, bypasses anyone who refuses to accede and labels them as suspicious. In the future, we can predict that states and individuals will generate a fog of incorrect data in an act of defiance designed to shield themselves from view.[38] Finally, digitalization is throwing up unexpected geopolitical changes. Ultimately, it will sweep away repetitive jobs and temporarily concentrate power in innovative territories, while making it possible for states and businesses to identify opinion leaders using relational mapping. Lastly, it will enable military chiefs to

[37] The lack of local training and a general lack of awareness of the dangers of cyberattacks have left the kingdom exposed.

[38] Voice cloning is now a reality. Using a single minute of recorded audio, Lyrebird and Wave Net can digitally recreate an individual's voice to have him or her "say" whatever they want. Similarly, Stanford University has demonstrated facial control in which a person's facial expressions are recorded live but edited by an actor, with a computer instantly reproducing the latter's movements yet with any target person's face. Such deepfakes can attack individuals, organizations, and states. University College London has developed its *My Text in Your Handwriting* program to accurately reproduce a person's handwriting from a single sample. A talking robot named Luka mimics the characters from the TV series *Silicon Valley*, recycling dialogue from the first two seasons. The robot responds to questions by generating new phrases based on the models provided to it. In 2022, it is believed that populations in developed nations will read more fake news than genuine information. Automatic text, image and audio generators could contaminate the entire human communication network. 8.5 percent of Twitter accounts are already run by bots.

order robots to kill targets using AI-powered facial recognition. We are entering into the era of hybrid civilizations.